Listing of Claims:

1. (Currently Amended) An electronic voting method, comprising the steps of:

obtaining from a signer apparatus, ~~using~~ according to a fair blind signature scheme, a digital signature (y_i) of a data signal (x_i) generated from a voter apparatus, said data signal comprising [[a]] an encrypted vote (v_i) of a voter; and

establishing, at a trusted authority apparatus, a link between ~~a given digitally signed data signal~~ a data pair (x_i, y_i) comprising said data signal and said digital signature, and a signing session in which said ~~digital signature~~ data pair (x_i, y_i) was generated, the fair blind signature scheme permitting establishment of the link via a tracing protocol included in the fair blind signature scheme.[[,]] ~~said trusted authority apparatus being enabled to establish the link via a tracing protocol included in the fair blind scheme~~[[.]]

2. (Currently Amended) The voting method of claim 1, wherein the fair blind signature scheme comprises a threshold fair blind signature scheme in which the digital signature is ~~obtained~~ generated by cooperation of a number t of n servers, where $t < n$, and where $n - t + 1$ servers need to be honest. ~~from a sub-set of a group of servers which form said signer apparatus, the group of servers containing n servers and the sub-set containing t servers, where $t < n$~~[[.]]

3. (Currently Amended) The voting method of claim 1, wherein the data signal (x_i) corresponds to the encrypted vote (v_i) of the voter which is encrypted according to a first encryption scheme (E_{TM}), said first encryption scheme being the encryption scheme of a first mix-net (TM) contained in a ~~voter-tallying~~ vote-tallying module.[[,]] ~~and the method further comprises the step of using said first mix-net (TM) to apply a decryption scheme (D_{TM}) which is~~

~~an inverse of said first encryption scheme to said data signal (x_i) at said voter tallying module to retrieve the vote (v_i) of the voter~~[[.]]

4. (Currently Amended) The voting method of claim [[20]] 3, ~~and~~ further comprising the steps of:

receiving from a voter apparatus, at a server module of said signer apparatus, a plurality of voter data (Id_i, C_i, e_i, s_i) during a voting process, one of said plural voter data (Id_i, C_i, e_i, s_i) comprising a signed blinded encrypted data (e_i) corresponding to the encrypted vote (v_i) of a respective voter (v), said vote being encrypted according to the first encryption scheme (E_{TM}), blinded by said voter, and digitally signed by said voter;

when the voting process has ended, publishing a voter data list (L_{AS}) of all voter data received from the voter apparatus;

during the voting process, receiving at a ballot-box module, from the voter apparatus, a plurality of ballot data (Id_i, C_i, c_i, σ_i), one of said plural ballot data comprising a signed encrypted data signal (σ_i), said signed encrypted data signal (σ_i) corresponding to the data signal (x_i) of a respective voter encrypted according to a second encryption scheme (E_M) of a second mix-net (M) contained in a vote-randomizing module, and digitally signed by said signer apparatus;

verifying the signature of said signed encrypted data signal (σ_i);

when the voting process has ended, publishing a ballot data list (L_{BB}) of all ballot data having a valid voter signature;

receiving, by a ballot-order-randomizing module, a batch of encrypted data signals (c_i) from said ballot-box module when the voting process has ended, said encrypted data signals being in a first order within said batch of encrypted

data signals (c_i);[[,]] ~~each encrypted data signal (e_i) comprising data encrypted according to a second encryption scheme (E_M) and said data including a respective data signal (x_i), the encrypted data signal (e_i) including the vote (v_i) of the voter subjected to plural levels of encryption~~[[;]]

retrieving, ~~in~~ by said ballot-order-randomizing module, in said batch of encrypted data signals (c_i), each respective data pair (x_i, y_i) ~~signal (x_i) from the respective encrypted data signal (e_i) in said batch of encrypted data signals (e_i)~~ by applying a second decryption scheme (D_M) which is an inverse of said second encryption scheme (E_M);

outputting, by said ballot-order-randomizing module, ~~the retrieved data signals (x_i) for said batch of encrypted data signals (e_i)~~ a data-pair list (L) of said retrieved data pairs (x^j, y_j) in a second order which is different ~~order~~ from said first order; and

receiving, by said vote-tallying module, said retrieved data ~~signals (x_i)~~ pairs (x_j, y_j) in said ~~different~~ second order.

5. - 8. (Canceled)

9. (Currently Amended) The voting method of claim 1, further comprising the steps of:

receiving said data signal (x_i) to be digitally signed ~~for the digital signature~~ according to said fair blind signature scheme at a server module of said signer apparatus, said data signal (x_i) comprising the vote (v_i) selected by the voter ~~(V_i)~~, said vote (v_i) being encrypted according to a first encryption scheme (E_{TM}), blinded according to said fair blind signature scheme and digitally signed according to a digital signature scheme of said voter;

verifying, by said server module, that the digital signature (s_i) of the digitally signed ~~in the received~~ data signal is valid;

in cases where the verifying step confirms that the digital signature in the data signal received by said server module is valid, digitally signing by said server module ~~digitally signs~~ the blinded encrypted vote (e_i) according to said fair blind digital scheme and ~~outputs~~ outputting by said server module a digitally-signed message ($S_{AS}(e_i)$);

unblinding the digitally-signed message ($S_{AS}(e_i)$) to yield said digital signature (y_i) of the data signal (x_i);

encrypting said data signal (x_i) and said digital signature (y_i) of the data signal thereof according to a second encryption scheme (E_M) to produce an encrypted data signal (c_i); and

signing said encrypted data signal (c_i) according to the digital signature scheme of the voter ~~(V_j)~~.

10. (Currently Amended) An electronic voting system comprising:

a plurality of voter modules each including a first processor; and

an admin server module including a second processor;

wherein the first processor[[, a]] of said plural voter modules ~~module~~ and the second processor in the admin server module cooperate during a respective signing session in application of a fair blind signature scheme to obtain, from said admin server module, a digital signature (y_i) of a data signal (x_i) from said one of said plural [[a]] voter modules ~~module~~, said data signal (x_i) comprising a respective vote (v_i) of a voter, said fair blind signature scheme having a tracing protocol which enables a trusted authority apparatus to establish a link between a

given digitally-signed data signal and a signing session in which said digital signature was generated.

11. (Previously Presented) A voter module including a first processor configured to cooperate with a second processor in an admin server module during a respective signing session in application of a fair blind signature scheme to obtain, from said admin server module, a digital signature (y_i) of a data signal (x_i) from the voter module, said data signal (x_i) comprising a vote (v_i) of a voter, said fair blind signature scheme having a tracing protocol which enables a trusted authority apparatus to establish a link between a given digitally-signed data signal and a signing session in which said digital signature was generated.

12. (Currently Amended) ~~A computer readable medium encoded with a~~ A computer program ~~executed by a computer that causes a~~ executing on a first processor which, when used on a computer apparatus, causes the first processor to cooperate with a second processor in an admin server module during a respective signing session in application of a fair blind signature scheme, the computer program comprising:

program code for obtaining, from said admin server module, a digital signature (y_i) of a data signal (x_i), said data signal (x_i) comprising a vote (v_i) of a voter; and

program code for establishing, at a trusted authority apparatus, a link between a given digitally-signed data signal and a signing session in which said digital signature was generated, said trusted authority apparatus being enabled to establish the link via a tracing protocol included in the fair blind scheme.

13. (Previously Presented) A voting system admin server module including a first processor configured to cooperate with a second processor in a voter module during a respective signing session in application of a fair blind signature scheme to obtain, from said admin server module, a digital signature (y_i) of a data signal (x_i) from said voter module, said data signal (x_i) comprising a vote (v_i) of a voter, said fair blind signature scheme having a tracing protocol which enables a trusted authority apparatus to link a given digitally-signed data signal with a signing session in which said digital signature was generated by said admin server module.

14. (Currently Amended) ~~A computer readable medium encoded with a~~ A computer program ~~that causes a~~ executing on a first processor which, when used on a computer apparatus, causes the first processor to cooperate with a second processor in a voter module during a respective signing session in application of a fair blind signature scheme, the computer program comprising:

program code for obtaining a digital signature (y_i) of a data signal (x_i) from said voter module, said data signal (x_i) comprising a vote (v_i) of a voter; and

program code for establishing, at a trusted authority apparatus, a link between a given digitally-signed data signal and a signing session in which said digital signature was generated, said trusted authority apparatus being enabled to establish the link via a tracing protocol included in the fair blind scheme.

15. (Previously Presented) A voting system ballot-order-randomizer module comprising a processor configured to provide:

input means for receiving a batch of cast votes, each cast vote comprising an encrypted data signal (c_i) comprising data (x_i) indicative of a respective vote (v_i) of a voter which is digitally signed according to a fair blind signature scheme,

said fair blind signature scheme having a tracing protocol which enables a trusted authority apparatus to establish a link between a given digitally-signed data signal and a signing session in which said digital signature was generated, each encrypted data signal (c_i) being encrypted according to a predetermined encryption scheme (E_M);

a mix-net (M) for decrypting said encrypted data signals (c_i) by applying a decryption scheme (D_M) which is an inverse of said predetermined encryption scheme (E_M); and

output means for outputting the decrypted signals of said batch of cast votes in an order different from the order of corresponding encrypted data signals in said batch of cast votes.

16. (Currently Amended) ~~A computer readable medium encoded with a~~ A computer program executing on a processor which, when used on a computer apparatus, ~~that~~ causes a voting system ballot-order-randomizer to randomize a batch of cast votes, the computer program comprising:

program code for receiving, at an input means, a batch of cast votes, each cast vote comprising an encrypted data signal (c_i) comprising data (x_i) indicative of a respective vote (v_i) of a voter which is digitally signed according to a fair blind signature scheme, said fair blind signature scheme having a tracing protocol which enables a trusted authority apparatus to establish a link between a given digitally-signed data signal and a signing session in which said digital signature was generated, each encrypted data signal (c_i) being encrypted according to a predetermined encryption scheme (E_M);

program code for decrypting, at a mix-net (M), said encrypted data signals (c_i) by applying a decryption scheme (D_M) which is an inverse of said predetermined encryption scheme (E_M); and

program code for outputting, at an output means, the decrypted signals of said batch of cast votes in an order different from the order of corresponding encrypted data signals in said batch of cast votes.

17. (Previously Presented) A voting system tallying module comprising a processor configured to provide:

input means for receiving cast votes, each cast vote comprising a data signal (x_i) digitally signed according to a fair blind signature scheme, said fair blind signature scheme having a tracing protocol which enables a trusted authority apparatus to establish a link between a given digitally-signed data signal and a signing session in which said digital signature was generated, each data signal (x_i) comprising a respective vote (v_i) of a voter which is encrypted according to an encryption scheme (E_{TM}); and

a mix-net (M) for decrypting said encrypted votes (v_i) by applying a decryption scheme (D_{TM}) which is an inverse of said encryption scheme (E_{TM}).

18. (Currently Amended) ~~A computer readable medium encoded with a~~ A computer program executing on a processor which, when used on a computer apparatus, ~~that~~ causes tallying of cast votes, the computer program comprising:

program code for receiving, at an input means, cast votes, each cast vote comprising a data signal (x_i) digitally signed according to a fair blind signature scheme, said fair blind signature scheme having a tracing protocol which enables

a trusted authority apparatus to establish a link between a given digitally-signed data signal and a signing session in which said digital signature was generated, each data signal (x_i) comprising a respective vote (v_i) of a voter which is encrypted according to an encryption scheme (E_{TM}); and

program code for decrypting, at a mix-net (M), said encrypted votes (v_i) by applying a decryption scheme (D_{TM}) which is an inverse of said encryption scheme (E_{TM}).

19. (Canceled)

20. (Currently Amended) The voting method of claim [[19]] 3, further comprising the steps of:

receiving from a voter apparatus, at a server module of said signer apparatus, a plurality of voter data (Id_i, C_i, e_i, s_i) during a voting process, one of said plural voter data comprising a signed blinded encrypted data (e_i) corresponding to the encrypted vote (v_i) of a respective voter, said vote being encrypted according to the first encryption scheme, blinded by said voter, and digitally signed by said voter,

when the voting process has ended, publishing a voter data list (L_{AS}) of all voter data received from the voter apparatus;

~~setting a time period during which voting is authorized;~~

receiving from the voter apparatus, at a ballot-box module, ~~communicating~~ a plurality of ~~encrypted~~ ballot data ~~signals (e_i)~~ (Id_i, C_i, c_i, σ_i), one of said ballot data comprising a signed ~~to a ballot box module, each of said plural~~ encrypted data signal (σ_i) ~~signals (e_i) including data from~~ corresponding to the

data signal (x_i) of a respective voter encrypted (c_i) according to a second encryption scheme (E_M) of a second mix-net (M) contained in a vote-randomizing module, ~~indicative of the vote (v_i) of said voter~~ and digitally-signed by said signer apparatus; ~~and~~

~~outputting, by said ballot box module, said encrypted data signals (e_i) to said vote-tallying module after expiration of the time period in which voting is authorized~~

verifying the signature of said signed encrypted data signal (c_i); and

when the voting process has ended, publishing a ballot data list (L_{BB}) of all ballot data having a valid voter signature.

21. (Canceled)

22. (New) The voting method of claim 3, comprising the steps of:

receiving from a voter apparatus, at a server module of said signer apparatus, a plurality of voter data (Id_i, C_i, e_i, s_i) during a voting process, one of said plural voter data comprising a signed blinded encrypted data (e_i) corresponding to the encrypted vote (v_i) of a respective voter, said vote being encrypted according to the first encryption scheme, blinded by said voter, and digitally signed by said voter,

publishing a voter data list (L_{AS}) of all voter data received from the voter apparatus when the voting process has ended.

23. (New) The voting method of claim 20, further comprising the steps of:

comparing, by the server module of said signer apparatus, the voter data list (L_{AS}) of all voter data received from the voter apparatus with the ballot data list (L_{BB}) of all ballot data; and

if there is an entry in the voter data list (L_{AS}) from which there is no corresponding entry in the ballot data list (L_{BB}), applying a signature tracing algorithm of the fair blind signature scheme to identify the data pair (x_i, y_i) which is in the voter data list (L_{AS}) and which has no corresponding entry in the ballot data list (L_{BB}); and

recording the identified data pair (x_i, y_i) in a revocation list (RL) containing ballots that have been rejected.

24. (New) The voting method of claim 23, further comprising the steps of:

receiving, by said vote-tallying module, a data pair list (L) of retrieved data pairs (x_i, y_i);

checking, at the vote-tallying module, said data pair list (L) of data pairs (x_i, y_i) for duplicate entries;

if there are no duplicate entries, checking a validity of digital signatures (y_i) of data pairs of the data pair list (L);

if the signature of data pairs of the data pair list (L) is valid, comparing data pairs (x_i, y_i) of the data pair list (L) with entries of the revocation list (RL);

if there is no data pair of the data pair list (L) in the revocation list (RL) decrypting the data signal (x_i) of the data pairs (x_i, y_i) by applying the decryption scheme (D_{TM}) which is an inverse of said first encryption scheme (E_M);

tallying decrypted data signals (v_i) corresponding to votes of the voters; and

publishing a voting result.

25. (New) The voting method of claim 24, further comprising, when duplicate entries are found, the steps of:

prompting the particular mix-server (M_j) to generate a zero-knowledge proof of correctness using the data pair (x_i, y_i) associated to a duplicate entry as input to a back-tracing protocol; and

if a particular mix-server generates a proof of knowledge, revealing an identity of a misbehaving voter by implementing a back-tracing algorithm of a randomizing mix-net, using the data pair (x_i, y_i) associated to the duplicate entry as input to the back-tracing protocol;

adding the data pair to the revocation list; and

removing the data pair from a list of votes to be counted.

26. (New) The voting method of claim 24, further comprising, when an invalid signature is found, the steps of:

prompting a particular mix-server (M_j) to generate a zero-knowledge proof of correctness using a data pair (x_i, y_i) associated to the invalid signature as input to a back-tracing protocol;

if the particular mix-server generates a proof of knowledge, revealing an identity of a misbehaving voter by implementing a back-tracing algorithm of a randomizing mix-net, using the data pair associated to the invalid signature as input; and

adding the data pair to the revocation list; and

removing the data pair from a list of votes to be counted.

27. (New) The voting method of claim 24, further comprising, when a data pair of the data pair list is found in the revocation list, the steps of:

prompting a particular mix-server (M_j) to generate a zero-knowledge proof of correctness using said data-pair (x_i, y_i) found in the revocation list as input to a back-tracing protocol;

if the particular mix-server generates a proof of knowledge, revealing an identity of a misbehaving voter by implementing a back-tracing algorithm of a randomizing mix-net, using said data pair found in the revocation list as input;

adding said data pair to the revocation list; and

removing said data pair from a list of votes to be counted.

28. (New) An electronic voting method, comprising:

obtaining from a signer apparatus, according to a fair blind signature scheme, a digital signature (y_i) of a data signal (x_i) generated from a voter apparatus, said digital signal comprising an encrypted vote (v_i) of a voter;

wherein the fair blind signature scheme includes a tracing protocol which can be implemented, at a trusted authority apparatus, to establish a link between a data pair (x_i, y_i) comprising said data signal and said digital signature, and a signing session in which said data pair (x_i, y_i) was generated.